Canning the Spam : Is There a Case for Legal Control of Junk Electronic Mail?

Lilian Edwards (1)

Go back to the AHRB Centre's publication section.

Few Internet users will not at some point have received an e-mail message of the following kind:

Subject: Fantastic opportunity!!!
From: makemoney@yahoo.com
MAKE MONEY THE EASY WAY!!!!
Your skills and experience can make you $$$$$$$ in only a few months. Send $50 dollars to Make Money Promotions to set yourself up in easy street for life. Go to http://www.makemoney.com/getajob/index.html for further details!!!

Such unsolicited or "junk" e-mails are colloquially known as spam(2). They are usually sent out to thousands if not millions of electronic mailboxes simultaneously, most often for dubious commercial purposes, though some are also sent by private individuals, for example to spread racist or homophobic hate speech. Spam can usually be spotted quickly by its use of multiple exclamation marks and capital letters (the Internet equivalent of shouting), or by enticing subject lines such as "get rich quick" or "hot sex here". Although most often found in the context of e-mail, Usenet newgroups can also be spammed, and for this reason LINX , the London Internet Exchange, has suggested a better description would be "unsolicited bulk material" or UBM. The presenting features of spam are that they advertise goods or services the recipient has not actively sought (typical examples being pornography, get rich quick schemes, pyramid selling schemes, dating agencies or software with which to become a spammer yourself), they are often misleading or outright fraudulent, very often offensive in content, and often arrive more than once to the same recipient. One problem may to be to separate "legitimate" bulk mailing from spam: is it simply a matter of volume or must these other criteria be brought into play? As we shall see below much of the harm caused by spam is simply a result of its bulk rather than its actual content. Organisations such as clubs and universities do send out mass e-mailing to eg their students, alumni, staff or sponsors - should such bulk mailings be classified as spam?

Almost all spam originates in the US currently, though this may change as UK entrepeneurs become more aware of the almost cost free opportunities of direct marketing by bulk e-mail. While spam has been very much in evidence ever since the Internet moved on from its earlier, quieter non-commercial incarnation (ie, roughly since the mid 1990s)(3)and has been the subject of much Internet user complaint and disgruntlement, there has until very recently been very little legal debate on how spam could, or should, be controlled in this country. By contrast there have for some time been active running battles in the US courts between spammers and those who would seek to stamp out the practice - notably Internet Service Providers (ISPs) - as well as a flood of proposed and in some cases, implemented state and Federal legislation intended to "can the spam"(4). UK interest is however now increasing (5) as spam is increasingly seen not just as a local annoyance to users but as a disincentive to the development of consumer confidence in the Internet as a commercial medium, and both the UK and the EC are now actively considering solutions to the problem of spam and whether existing or new legislation can be an effective tool to control it (6).

Why should spam be subject to regulation?

The historic response to spam has been to regard it as a nuisance, and perhaps to take self help measures such as "flaming" (sending abusive e-mails to the spammers) but not as a fit subject for legal (or extra-legal) regulation. However a number of factors have conspired to make it a subject that is worth taking seriously.

Most obviously, spam is annoying and in some cases, offensive, to its recipients. Worse still, traditional direct marketing is usually only directed at solvent adults, while spammers will indiscriminately spam children and other vulnerable groups so long as they have an e-mail address(7). From a legal perspective, spam is an invasion of the privacy of the individual whether the mail box is situated at home or work. Spam has been described as combining the worst aspects of junk mail, telephone solicitation ("cold

calling") and junk faxes(8). In this aspect, spam is not dissimilar to traditional, non electronic direct marketing, although it is significant that the costs of marketing by spam are shifted almost wholly from the spammer, to the recipient who pays his ISP for downloading time (9) .

"Spamming" however has serious consequences other than irritation for the recipients of the message, and also has economic implications for persons other than the recipient. It is the financial detriment spam potentially causes which has arguably created the most compelling public interest in the prevention of spam. In the EC especially, the main current concern in this area is that spamming fundamentally impedes consumer confidence in the Internet as a safe and serious commercial medium, rather than one full of sharks, wide boys and fraudsters (10). In this respect the European debate around spam is similar to that around the regulation of encryption and pornography(11): in both cases, the public interest in protection from offensive content, or protection of privacy rights, carries less weight than the economic argument that unless the Internet is cleaned up and made secure for consumers and businesses, electronic commerce cannot thrive (12). Furthermore, because so much spam fails to meet fair trading and honesty standards (13), "legitimate" adverts from reputable advertisers are almost always ignored or deleted, or attempts are made to filter it out by the system administrator. Effectively, the result is that the Internet cannot be used sensibly for legitimate direct marketing currently.

Certain particular groups suffer direct economic losses as a result of spam. Some well known ISPs with a large client base whose e-mail addresses can be easily "harvested" by acquiring a temporary guest account, tend to be heavily spammed, eg AOL and CompuServe, and this causes them to lose custom as users become annoyed with receiving spam and leave and subscribe to another ISP (it should be remembered that the ISP market is a highly competitive one where users tend to show little brand loyalty). Users waste on-line time, which despite the growth of free ISP services in the UK, is still often charged on an hourly basis (plus local call costs), downloading, reading and deleting spam. Employers also suffer additional costs, as spam wastes employee time, both in examining and deleting spam, or by becoming frustrated and replying to it . A report commissioned by Novell in April 1998 concluded that junk e-mail was costing UK industry £5 billion per year (14).

Finally and perhaps most importantly, spam threatens the efficiency and speed of the Internet for all users. The sheer bulk of traffic sent out by spammers - who use special spamming software to sometimes send tens of millions of messages at one go - congests the Internet, using up bandwidth and slowing down, not just e-mail, but also other services such as the Web. Servers from which spam is sent, or to which or through which it is transmitted, may crash, not just as a result of the initial volume of mail sent out but because of "mail undeliverable" messages returned from inaccurate e-mail addresses. ISPs tend to buy only as much bandwidth as they need to support the estimated traffic of their subscribers and massive surges of use caused by spammers will either crash the server or require the ISP to waste money buying excess bandwidth as preventative strategy. This again represents a major problem to ISPs and their system administrators who to retain customer confidence need to provide 24 hour access and keep networked workplaces going (15). In one recent US case (16) , the court estimated that the real costs to an ISP of dealing with each spam message were 0 .078 cents per message. Since in that case 130 million junk e-mails were sent, the court awarded US$400,000 dollars against the spammer (including a punitive triple multiplier on the estimated damages). In another case it was estimated that handling spam had so degraded the performance of the server afflicted by spamming that e-mails that should have been delivered in minutes were taking three days to arrive (17) .

Ways to stop spammers

Having perhaps established that spam is a problem worthy of regulatory concern, how , if at all, how can it be stopped? The naïve or perhaps the optimistic among us might think that the simplest thing in the world to do would be to ask the spammer to simply stop annoying us. Spam messsages, like all e-mails, carry a return address. Indeed, most spam messages do include a line to the effect of "If you wish to receive no more mail from this address, please reply to nospam@spam-domain.com". The many users who take this up as a genuine offer tend to discover however that the return or reply-to address is nearly always fake (18) , resulting in an undeliverable mail message. This has three advantages for the spammer; one, he is not deluged by a flood of complaints from the spammed population; two, he is effectively untraceable so that he can avoid having legal writs served on him; three, the spammer can use your reply to the "nospam" address to ascertain that the e-mail address spammed is indeed valid (which sometimes, to add insult to injury, may result in the address so validated being offered for sale to other spammers or direct marketers). So if asking for direct removal from a spammer's list is unlikely to work, then other solutions - legal or extra-legal - must be explored. Below are canvassed some suggestions for ways in which both law and technology can be harnessed to help prevent spam.

As was noted above there are a number of persons who may suffer from spamming - individuals who

receive it, ISPs who handle it, and the general public who absorb the costs and ill will it creates. Legal action by victims of spamming will generally have one or both of two goals: one, to stop the spammer by closing down the ISP account the spammer is using; and two, to recover damages. An underlying goal for ISPs especially, is publicity : to make it plain that spamming is not something they will tolerate in the best interests of their customers. The public interest in removal of spam may also be sufficient to justify invoking the criminal law.

Can civil liability be imposed on spammers?

1. Contractual Claims

   For a spammer to go about their work, they must have access to the Internet. This will require the formation of a contract for the ongoing or temporary services of an ISP. Many ISPs insert as standard provisions in their subscriber contracts that spamming is regarded as a fundamental breach allowing the contract to be terminated unilaterally by the ISP at any time (19) and even where there is no express anti-spam clause, it is possible that the courts would be prepared to accept it as a term implied by the common practice of the business of providing Internet access (20).

   In many US ISP contracts, furthermore, a system of rising penalties is also put in place for repeated spamming, which may be imposed as well as or instead of, termination of the contract. The problem with provisions of the latter type is that in both Scotland and England, such might be struck down as illegal penalty clauses, rather than as true liquidated damage clauses (21) . There might also be some difficulty if either termination or penalty clauses were to be contested as unfair ; as ISPs invariably only offer standard form contracts to subscribers, terms imposed by such would be subject to scrutiny both under the Unfair Contract Terms Act 1977 (UCTA77) and the Unfair Terms in Consumer Contracts Regulations 1994. A challenge however might be mounted to the applicability of the 1994 Regulations on the basis that a spammer signing up for an ISP account is not a "consumer", but someone acting in the course of business. (22) In any case, the question is often academic, as spammers tend to gain access to the Internet by using free and transient guest memberships, often giving false identifying details, and then moving on speedily to the next account. In such circumstances, contractual remedies tend to be of little avail. However it is noteworthy that the first UK writ served against a spammer, one Adrian Paris, was raised by Virgin under two grounds one of which was breach of contract (23) . (The case was settled in June 1999 for £5,000).(24) The case was however unusual in that Paris (remarkably) had subscribed to Virgin under his true identity (25) .

   As we saw above, it is not always the ISP with which the spammer has a contractual relationship which alone suffers financial loss. Where can we find remedies for those affected economically by spamming activity who either do not have a contractual relationship or cannot rely on an appropriate contractual term?

2. Claims in Tort or Delict

   The US courts have several times allowed claims in tort against spammers by ISPs whose service to their client base is degraded by spam e-mails. The basis of such actions is usually the tort of trespass, which under the US Restatement can be established where intentional damage is done to the moveable property of the service provider (26). One successful US trespass case was *CompuServe Inc v Cyber Promotions* (27), the case cited above, in which CompuServe's server's performance was so degraded that e-mail took three days to deliver which would normally have taken minutes. In that case, the US District Court of Eastern Ohio had little difficulty in finding that damage caused by electronic signals could be sufficiently tangible to found the tort; that the damage caused to the plaintiff's property did not need to be permanent so long as it had resulted in actual impairment of its quality or value; and that CompuServe had not given permission to any use at all the spammers made of the Internet access they offered simply by forming a contract for ISP services with that person.

   It is difficult, unfortunately, to see how these US cases could be applied directly to Scots law though there may be a possibility of such an approach succeeding in England, where the law on trespass to moveables is not dissimilar to that in the US Restatement (28). In the English *Virgin* case cited above (29), the second head of action was trespass. In Scotland, however, the law of trespass is considerably narrower than in England, and the delict of trespass relates almost exclusively to use without permission of heritage (land and buildings). It seems that trespass can

only be an actionable delict in relation to moveables such as cars or ships, which can be occupied (30). The tort of conversion is also unknown in Scots law. A general action for interference with moveable property on the grounds of culpa would seem possible, as culpa is sometimes seen as covering both intentional and unintentional conduct so long as loss is caused to another - but the difficulty then arises that the loss to an ISP may well be wholly purely economic, for which the courts are generally reluctant to allow recovery (31). As we have seen, even servers put out of commission by spam recover without any permanent damage, and losses based on client dissatisfaction are clearly purely economic.

A more workable possibility might be to seek damages on the basis of what are known as economic torts or delicts: eg that the spammer has interfered with the ISP's performance of its contract with its clients to provide them Internet access(32), or , more broadly still, that the spammer has wrongfully interfered with the ISP's business (33). The law relating to such economic delicts in both Scotland and England is however not at all clear on a number of points, eg does the spammer have to have *intended* to interfere with the ISP's contractual performance or business, or will his recklessness about this likely consequence do? Does the spammer's interfering act, ie, sending spam, itself have to be an unlawful act even before it interferes with the ISPs activities? Can the restraint of one party's business activities be justified merely because it interferes with another party's business - or is it legitimate competition, even though spammers and ISPs have quite different trades? A court appraised of how damaging spam can be, is perhaps unlikely to be sympathetic to the spammer in these regards but the uncertainty may still impede legal claims. Even if a claim was allowed in principle, uncertainty persists about what heads of damages would be accepted by a UK court as sufficiently proximate (direct losses suffered due to server shutdown, general loss of goodwill, loss of reputation, customers switching ISPs, slowdown in ISP performance?).

3. Trademark Infringment

Where well known brands are spoofed within the main text of the messages sent by spammers, or, more interestingly, a well known ISP name is given as part of a fake or "spoofed" reply-to address, then claims for trademark infringement or passing off may arise (as may a common law action for fraud). The argument in the latter situation is that recipients will be confused into believing the messages were sent out with the complicity of the spoofed ISP when they were not, and so their trademark is infringed (34). In the US case of *AOL v Prime Data Systems* (35), spammers sent out 130 million junk e-mails all of which gave their reply-to address, fraudulently, as from the domain *aol.com*. The court found that there was wilful trademark infringement and awarded US$400,000 damages. American ISPs have found this a particularly attractive remedy in that it sends a signal out to the public, spammers, and subscribers alike, that "attempts to piggyback off [the ISP's] name" (36) will be vigorously repelled.

Can criminal liability be imposed on spammers?

1. The Computer Misuse Act 1990

The Computer Misuse Act 1990 (CMA) was introduced primarily to deal with the perceived vice of computer hacking (37). It was never anticipated during its drafting that it might be used to deal with junk e-mail. However in one informally reported case (38), an ISP known as Colloquium had its system brought down by an overload of spam causing downtime, loss and interference with its business - some 300,000 messages per hour were sent out by the spammer using its server. Unusually, the spammer was not only resident in UK but was an ex-customer of the ISP and had given it his correct name and phone number. Strathclyde Police investigated and the possibility was raised of charges under the CMA, although it is not clear under what provisions, or indeed if any prosecution subsequently transpired.

Does the CMA provide a means, as the operator of Colloquium suggested, to "make a junk mailer think twice"? The problem with this approach is that the sanctions provided by the CMA are not really tailored to deal with a legitimate user who then abuses Internet access provided, but rather with an unauthorised or intrusive user. Use of an account with an ISP to send spam, where the contract expressly or impliedly states that spamming is forbidden, may, taking a common sense approach, appear to be "unauthorised" access under s 1 of the Act and thus criminal. However *DPP v Bignell*(39) makes it clear that so long as the *access* to the server has been authorised - which it will have been if the spammer has lawfully acquired some kind of legitimate ongoing or guest account - then a s1 offence is not committed whatever *purpose* the access is then used to

secure. In *Bignell* itself, a policeman was given legitimate access to the Police National Computer - but then used this access not for the proper purposes of his job, but for an unauthorised purpose, namely finding out personal details about his estranged wife. It was held that no s 1 offence had been committed. This result is a particularly unfortunate one since a s 1 offence must be established as a prerequisite to prosecution for more serious offences, with heavier sentences, under s 2 of the Act.

Section 2 is known as the "ulterior intent" section and provides that an offence is committed where anyone commits the s 1 offence with the intent to commit or facilitate the commission of another offence to which the section applies. So for example, if (as is often the case) the spam itself contained statements that were criminally fraudulent, s 2 would allow for a penalty of up to 5 years' imprisonment or a fine to the statutory maximum to be imposed so long as "unauthorised" access under s 1 could be established. *Bignell* however currently blocks this approach (although straightforward prosecution for fraud would still be available).

A final possible ground of prosecution under the CMA may be found in s 3, which provides that an offence is committed if anyone with deliberate intent (40)causes an "unauthorised modification of the contents of any computer". Section 17(7) defines such a modification as taking place if *either* any program or data held on the computer concerned is altered or erased, or any program or data is added to the contents of the computer. The modification must *then* be intended to (a) impair the operation of the computer; or (b) to prevent or hinder access to any program or data held on any computer; or (c) to impair the operation of any such program or the reliability of any such data (s 3(2)).

Again, we have the problem that these provisions were clearly drafted to catch the disseminators of computer viruses or logic bombs, not direct marketers. To fit the facts of spamming into s 3 requires extremely convoluted interpretation. In the Colloquium case, it appears that the server crash mainly occurred because "mail undeliverable" messages, returned due to inaccurate e-mail addresses being used by the spammers, were "added" to the ISP's server. Can s 3 apply? Three problems arise. First, are return e-mail messages "data"? They are certainly not programs (41). No definition of data is given in the Act (deliberately), so, perhaps (42). Secondly, even if adding e-mail messages to the server is seen as a "modification", again we have the *Bignell* problem of whether it is an "unauthorised" modification if the spammer had legitimate access to the e-mail program provided by the ISP (and to storage space on the server)(43). Again, there is some possibility *Bignell* might be distinguished in this context, since the issue here is whether the *modification* was unauthorised, rather than the *access*(44). But the main stumbling block is that the spammer clearly did not *intend* to create any of the impairments described in s 3(2). He merely intended to send out spam. It seems unlikely that his mere recklessness as to other possible results, including server crashes, or even interference with services ("program"s) provided to ISP clients, while he carried out this primary intention, would be enough to found criminal liability.

Although this result is unfortunate from a spam point of view, it makes perfect sense given the intention of the legislators. Any forced interpretation which allowed spammers to be caught might also allow, say, any innocent user who sent an e-mail or used a program in some way which inadvertently caused a system crash to be tried under s 3. Every local area network user knows that modern computer systems are, unfortunately, still very fragile. Given the debate about whether even intentional computer virus creation and dissemination is a serious enough issue to deserve criminal penalties, it seems unlikely a court would bend over backwards merely to criminalise the activities of unscrupulous direct marketers without taking cognisance of possible side effects.

2. Alternative criminal remedies

As we have already mentioned, some (though not all) spam may be criminally fraudulent under English statute (45) or Scottish common law. In addition, the Telecommunications Act 1984, s 43 makes it a criminal offence to use a public telecommunications network to send "grossly offensive, threatening or obscene" material, and a "public telecommunications network" is widely defined enough to cover Internet traffic which goes through phone lines or other cables. Thus we have a partial remedy for at least that portion of spam which is criminally offensive or deceptive. The outstanding problem however, from the Scottish or English perspective, is that most spam currently comes from the US and thus, criminal jurisdiction being territorial, the spammers will probably fall outside the jurisdictional and enforcement capabilities of the UK authorities. We shall return to the difficulties of enforcement below.

Remedies for the recipients of spam?

Data protection law

Given this, and the apparent inadequacy of the civil and criminal remedies canvassed so far, perhaps it is better to try another approach. So far we have mainly focused on
(i) sanctioning the person who *sends* the spam, and (usually simultaneously)
(ii) providing financial compensation for ISPs who are economically hurt by their activities.

We now turn however to seeking to protect the members of the public who are spammed. As noted above, apart from the question of offence and alarm, the main impact on the public of spam is that of annoyance, invasion of privacy, and generally of loss of confidence in the Internet as a lawful and honest medium. The response to ordinary direct marketing as a nuisance factor in the EU has mainly been to look at protection of personal data, an idea which springs fundamentally from the European Convention on Human Rights' protection of the individual's right to privacy (46). (In the US by contrast it has been accepted, albeit with some reluctance that direct marketing is a form of speech and as such protected by First Amendment rights, although the protection given is less than that which would be accorded non-commercial speech)(47). European protection originates in the activities of the Council of Europe, who in 1981 passed a Convention on Automatic Processing of Personal Data which was incorporated into UK law by the Data Protection Act 1984, one of whose main purposes was to control the unauthorised transfer of personal data held on computers for the purposes of direct marketing. More recently the EU has passed a Data Protection Directive of 1995 (48) which required all member states of the EU to implement it in national law by 24 October 1998 (although in many states, including the UK, that deadline has not been met). In the UK, the revised data protection law is now to be found in its entirety in the Data Protection Act 1998 (49)

The first question is whether spammers come within the remit of the 1998 Act at all. The Act is less than crystal clear in its drafting (50), but speaks of "data controllers", who are under a statutory duty (i) to comply with the Data Protection Principles (51) and (ii) to register with the Data Protection Commissioner ("notify" within the 1998 Act terminology) as persons who are processing personal data (52). If these duties are breached, then the data controller may be liable to compensate any individual adversely affected, even if the Commissioner does not serve an enforcement notice (53), and criminal liability may also be incurred (54).

The first question then is whether spammers are "data controllers". A data controller is " a person who… determines the purposes for which and the manner in which personal data are, or are to be, processed. (55)" This begs the question, do spammers process "personal data"? Typically, spammers harvest from newsgroups, web sites or ISP mail programs, buy, or otherwise obtain, long lists of personal e-mail addresses, to which a spam e-mail is then sent by special software. Under s 1(1)of the 1998 Act, "Processing" includes "…carrying out any operation on the information or data", which seems to fit these activities satisfactorily. However the meaning of "personal data" itself may be more problematic. Section 1(1) defines personal data as "data which relates to a living individual who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or likely to come into the possession of, the data controller." Does an e-mail address, without any other added information, identify an individual, in the same way that a name and physical address would? Some may seem to, others may not. This writer, for example, maintains e-mail addresses both as *Lilian.Edwards@ed.ac.uk* and *eusl01@law.srv0.ed.ac.uk.* At first blush, one might think the first address might be "personal data" since it reveals a person of female sex who probably works or studies at Edinburgh University, and the second not - an absurd result in itself - but the matter is complicated still further by the additional qualifier that data may be "personal" if it allows identification of an individual when combined with other information which is "*likely* to come into the possession of the data controller" (italics added). On the Internet, identifying information about many persons is easily obtainable simply by putting their e-mail address into one of the many search engines available. However, Gringras (56) points out that simply because such additional information is *easy* to obtain, does not mean that it is *likely* a spammer would obtain it, as his principle aim will be to send out spam, not to research the character of its recipients (57). The point remains however that given the use of search engines and other Web based aids, an e-mail address makes an Internet user "identifiable" and nothing in the Act requires that "personal data" must provide the actual *name* of the individual or "data subject" to which it pertains.

If the 1998 Act does apply to spammers, it is clear that on most occasions, they will be *prima facie* in breach of the 1998 Act in multiple ways. For example, spammers typically fail to register with the Data Commissioner as required, and also usually fail to meet the requirement of the First Data Protection Principle, that the consent of data subjects to the processing of their data must be obtained. Admittedly, such consent is not required if one of the other exemptions in Schedule 2 is applicable, but the only one that seems relevant to spam is that the processing is "necessary for the purposes of legitimate interests

pursued by the data controller" which interests must be balanced against the data subject's rights, especially to privacy (58). If the processing is detrimental to the interests of the data subject, as it arguably will be in the case of spam, then Carey (59) suggests the exemption is unlikely to exculpate the data controller. Spammers also typically fail to comply with the right of the data subject under s 11 to demand to cease receiving direct marketing (60) from the data controller in that they usually provide a spurious reply-to address for such requests(see above).

However all of the above is interesting but of little avail, given that the Data Protection Act only operates in the UK, and the 1995 Directive within the European Economic Area (EEA), when overwhelmingly, spam emanates from the US. (These remedies may of course become more useful once the local marketers do jump on board.) Although the jurisdictional provisions of the 1998 Act do perhaps extend to cover data controllers established outside the EEA who use "equipment" in the UK for "processing" the data (61) (are the servers and networks through which e-mail is routed "equipment"? Does the spammer use them for "processing"?) the problem still remains that enforcement of the data protection principles by EC nations effectively ends outwith the EEA (62). Spam is inherently a global problem not just (or even mainly) an EC one.

It is also worth noting that the scheme of data protection is inherently regulatory, rather than designed to provide remedies to individuals. As noted above, individuals can pursue civil claims against those who break the 1998 Act rules, and criminal prosecutions may in some cases be brought. But the main enforcement apparatus of the 1998 Act is the enforcement notice (63), which is served as a "last chance warning" on a malfeasant by the Data Protection Commissioner, with the intention of securing, if at all possible, compliance without criminal proceedings. In other words, data protection law is better seen as a way of creating a commercially cleaner Internet for the public to enjoy, than as a means of getting private remedy or revenge.

Consumer rights

Similar problems attach to other consumer remedies which may be relevant to protection from spam, and which will or may become available under the general umbrella of EU consumer protection. One of the more promising provisions is that EC consumers are to be guaranteed the right under the EC Distance Selling Directive (64) (which was to have been implemented in the UK by 4 June 2000)(65) not to receive unsolicited communications relating to distance selling where there is a clear objection from the consumer (66) The Directive is clearly intended to cover communications sent via the Internet as well as conventional mail and phone communications. (67) Although the UK is still consulting on the exact form of the regulations which will implement the scheme (68), what was first envisaged was that a register, printed or electronic, would be held under the supervision of OFTEL, which would record the names of individuals who positively asked not to receive distance selling communications : in other words an "opt-out" regime. Direct marketers were to be compelled to search this register in order to remove any such opting-out consumers from their lists before sending out communications. The more recent consultation paper issued by the DTI in November 1999 however took a more ambiguous line, with draft regulations being supplied which contained alternate opt-out and opt-in schemes (69). An "opt-in" scheme would mean that consumers would actually have to express a preference to receive unsolicited communications from the business in question before it would be legal for them to be sent such communications. Such an approach is generally seen as more effective at controlling spam (see further below). The Distance Selling Directive is however limited in relation to curtailing spam in that financial services are excluded from the Directive (and much spam involves financial scams)(70) as are business to business communications (which may cover almost all spam if commercial spamming is accepted as a business).

Another analogous source of remedies may be the Telecomunications (Data Protection and Privacy) (Direct Marketing) Regulations 1998 (71), which implement in the UK the direct marketing provisions of the 1997 Telecommunications Data Protection Directive (72). Currently, Art 12 of this Directive deals with unsolicited telephone calls and is aimed at cutting down on such "cold calling" against the wishes of consumers. Although the Directive gave states discretion to implement the Directive using either an "opt-in" or "opt-out" system, the DTI chose after consultation to opt for the latter, so that those who wish not to receive unsolicited calls will have to register to this effect. Breach of the Regulations is to be enforceable in the same way as breach of the Data Protection Act 1998, discussed above.

The DTI made it clear during the consultation period that the Regulations, and in particular, the word "calls", are not intended to extend to e-mail solicitations (73). However more recently, while consulting generally on issues surrounding electronic commerce (74), the DTI have suggested that one way forward on the problem of spam might be to extend these Regulations expressly to cover e-mail.

There are two clear problems, however, with both the existing Distance Selling protection and the

possible extension of the Telecoms Regulations. First, the difficulties of enforcing EU rules against predominantly American spammers are as compelling here as they were in relation to the Data Protection Act. Secondly, even if there were some kind of practical co-operation from the US in enforcing these rules, an "opt-out" regime - which both sets of rules envisage - is of very little practical help. Human nature is such that even faced with a constant source of annoyance, very few people are equipped to find out that a regulatory scheme exists which may help them, and even fewer will then make the effort to register their veto on spam. Most independent (ie not connected with the direct marketing industry) commentators agree that an opt-in scheme for spam would be more appropriate, under which consumers would have to indicate (bizarrely) their actual *desire* to receive spam. This is particularly so given that the Distance Selling Directive already prescribes a mandatory "opt-in" regime for junk faxes and automated calling machines (75), which repetitively contact certain telephone numbers and then either play a pre recorded message or connect the consumer to a human salesperson when the call is answered. The reason why these means of selling are distinguished from ordinary distance selling is, in the case of faxes, because the costs of marketing are transferred from seller to recipient, and in the case of automated calling machines, because of the extreme aggravation they cause. Both reasons apply to spam, and therefore it seems remarkable that the DTI has not so far taken the opportunity given to unambigously prescribe an opt-in regime for spam (76).

It should also be noted that "opt-in" is rather easier to achieve in relation to business-to-consumer (B2C) e-commerce than traditional distance selling. Any consumer who buys something from a web site can be offered a box to click if they want to "receive further information". This would do as "opt-in" ; there is no need for it be done via a central register as with "opt-out", so for small businesses, "opt-in" may actually be a cheaper regime under which to operate than "opt-out" where search fees will be a significant overhead. A final problem with "opt-out" regimes is that spammers in the US (who have already shown they are generally undaunted by law in the UK or EU in relation to data protection) may well just see a list of customers who have "opted out" as a list of particularly tempting targets - to put it bluntly, since these people presumably tend not to receive traditional junk mail or EC based spam (77), they will be fresh meat for US based spam . No doubt any list of consumers opting out from spam will in theory be held securely, but since it will have to be made available to spammers to fulfil its purpose - so that they can strike opt-outs from their mailing lists - how long can it be before it is circulating the Net or publicly available on a web site?

Finally there are some rather toothless proposals relating to commercial communications in the EC Electronic Commerce Directive, Arts 6 and 7, which has recently made its way through the co-decision procedure of the European Parliament and was finalised on 8 June 2000 (78). First, commercial communications must be "transparent" in the sense that certain information must be compulsorily available which identifies the sender, adequately discloses the nature and conditions of promotional offers made by the communication, etc (79). Secondly, *unsolicited* commercial communications must be "clearly and unambiguously" identifiable as such as soon as they arrive. The obvious way to implement such labelling in the case of spam at least is by requiring a word such as "advertising" to appear on the subject line of any spam e-mail. It is dubious how useful such a provision is, and when the DTI suggested it as one of the options for dealing with spam in its consultation document on promoting electronic commerce (80) there was little enthusiasm for it from respondents (81). Labelling may spare the sensibilities of recipients who are spared the experience of opening a message labelled (say) "Advertising: red hot porn", but will do little for the more economic problems caused by spam discussed above, eg, the on-line time they waste being downloaded and deleted, and the clogging up of Internet bandwidth. Labelling *will* give email filtering systems a tag to act upon , but may also interfere with users forwarding spam to ISP postmasters and other spam "vigilantes" so that they can be "blacklisted" (see below) as they are currently encouraged to do. And as for the general transparency requirements, why again would spammers, especially those from outwith the EC, comply, when they have generally failed to follow any other rules or business etiquette? Enforcement will certainly require, even within the EC, a considerable budget for investigation, given the ease of falsifying one's origins on the Internet, something which is exacerbated further by the current growth in Europe of free ISP accounts. What is most noticeable in Arts 6 and & is the absence of any decision by the Commission and Parliament to enforce the implementation of "opt-in" regimes. Art 7 provides merely that states must "respect the opt-out registers"; although since the E Commerce Directive is a minimum harmonisation this still leaves it open to individual states to implement more stringent regimes if they so wish.

The Future?

So far we have surveyed a rather gloomy terrain upon which legal solutions to the problem of spam present themselves, and then, like ghosts, fade away when confronted with the spectre of enforceability. We seem to be at the stage where everyone knows there is a problem, but no one knows what to do. As noted above, the DTI made tentative efforts in March 1999 to suggest a number of solutions to spam in its

consultation document on promoting electronic commerce, but reached the dispiriting conclusion that the problem should be left at the moment for industry to resolve, although the government would retain a watching brief and might be required to muster a legal response to deal with persistent offenders (82). The EC Commission and Parliament are also well appraised of the problem, but so far have done little more to address it than subsume the problem into the general issues of consumer protection and regulation of commercial communications, despite some last minute efforts by MEPs during the Parliament reading of the Draft E-Commerce Directive to add an amendment which would have banned unsolicited spam altogether (83). These interventions have in the end resulted only in an enabling provision which enjoins member states to take measures to ensure that *"service providers"* provide means by which consumers can register their desire to opt out from unsolicited commercial communications. "Service providers" are defined in Art 2 of the Directive as natural or legal persons providing an "Information Society service", which essentially means any service provided commercially at a distance via electronic equipment or networks, at the individual request of a customer. In other words, states are not being enjoined themselves to provide an opt out scheme; instead responsibility is being passed, it seems, to spammers and to ISPs to "self regulate" the spamming industry. This is a predictable response, given the EC's current action plan in relation to unwelcome Internet content control generally (84) but is again of dubious utility. How exactly are ISPs to know without constant monitoring (specifically not required by Art 14 of the Directive) whether spammers using the ISP are respecting any opt-out register, however collected? How are non-European spammers to be cajoled into respecting opt-out registers at all, as discussed above? And in any case, the objections raised generally to opt-out as opposed to opt-in schemes above apply *passim*.

As Dickie notes (85), although the EC does have a longstanding commitment to consumer protection, at the moment in terms of *Internet* regulation, the dominant focus seems to be liberalisation of the market, inspired by fears that over-regulation will impede European industry in its drive to catch up with the US in the development of e-commerce. Similar trends can be seen in the UK (86) in the DTI's approach to Internet regulation. All this, combined with the globalised nature of the spam problem, seems to have conspired to leave both consumers and ISPs as disempowered victims of spam.

This lies in odd contrast to developments in the US, which has also in recent years leant towards light-handed regulation of the Internet industry. Despite this liberal tendency, there has been a flood in recent years of US state legislation specially tailored to deal with the spam problem and a number of federal proposed statutes are also working their way through the legislative process (87). At least 18 states have enacted anti-spam legislation to date. The best known state statute is probably that passed by Washington State in March 1998 (88) which not only makes it an offence to send unsolicited e-mail and to provide a false reply-to or origin address, but also provides civil remedies of damages for actual harm caused to an ISP or recipient (89). The Californian Internet Consumer Protection Act, which came into force in January 1999, has in addition the interesting approach of pointedly giving teeth to anti-spam clauses imposed in ISP contracts by authorising ISPs to sue violators for damages for $50 per message, to a maximum of $25,000 per day (90). It is possible that the US has taken the route of statutory control of spam, not least because there is at least a fighting chance of being able to find and sue or prosecute the spammers there. Many state spam statutes have provisions exerting jurisdiction over persons outwith the state who send unsolicited e-mail to residents within the state, and clearly a Federal statute would be able to provide country-wide sanctions. But the US is also disadvantaged in terms of legislating for spam in that statutes have to be tailored narrowly to withstand the challenge that the government is restricting the First Amendment and Commerce Clause rights of spammers (91), while the EU in this area is only largely impeded in its competence by the issue of freedom of movement of commercial communications within the single market (92). In fact both of the US statutes mentioned above have been declared invalid as contrary to the First Amendment (subject to possible appeals) during the course of writing this chapter, a fascinating example of a legal system divided schizophrenically on how to regulate the Internet (93).

Within the knowledgeable Internet community itself, there is a fair degree of consensus that the best results will come not from legal regulation at all, but from "self regulation" by technical strategies or fixes (94). There are a number of less or more successful approaches. The first line of defence is that ISPs, local network managers, and individual users can use filtering software to remove e-mails sent from the addresses of known spammers. This however is only ever partially effective as the addresses of spammers change constantly (using guest, free or anonymous accounts), and are in any case usually disguised. There is some degree of co-operative "blacklisting" of sites and ISPs known to harbour spammers : one such blacklist often consulted by system administrators is known as the Real Time Black Hole List and is available on the Web (95). Traffic coming from a blacklisted site will not be transmitted on via other networks or ISPs where administrators have consulted the blacklist, with the effect that the black-listed site becomes isolated from the rest of the Internet. However no such system is foolproof, and a site which is being made use of by spammers against its own policies, or one which is sending out multiple copies of an e-mail for a valid reason (eg an alumni e-mailing from a university) may find itself black-listed alongside the "guilty" sites (96). It has been suggested that mistaken placing of a site on the list might be seen as libellous, which also provides a disincentive to co-operate in providing information to the

organisers.

Another simple mode of protection which is becoming commoner with the advent of more sophisticated e-mail programs (97)is to restrict the number of people who can receive a copy of a single message. Again however this can be counter-productive when there are legitimate reasons to mail a large number of people at once. Sophisticated e-mail servers can also be configured to notice any difference between the true origin of an e-mail message and a fake "repy-to" address in the message header. It is not then difficult to filter out all mail with fake reply addresses on the basis that it is almost certainly spam (98). Finally both ISPs (99) and networks increasingly have "acceptable use" policies which prohibit spamming. For example, JANET, the UK academic network, has a policy that its network cannot be used for the transmission of unsolicited commercial or advertising material (100). Such policies, like laws, are difficult to enforce against determined spammers (every UK academic, it has to be said, still receives spam), but they well be a useful disincentive to spammers of a more amateur variety and will open the door to sanctions of a local nature such as suspension of user accounts.

This article began by asking if there was a case for legal regulation of junk electronic mail. In this concluding paragraph, it seems that although a case can be established, the legal solutions currently available may be at best only moderately effective and at worst either ineffective or actively counter productive. Although technical solutions may offer the best current hope of a practical solution, this should not be seen as a blanket excuse for governments in Europe to opt out of their responsibility to help clean up the Internet for both private users and businesses. Nor can they expect the problem to go away simply by packaging it off to be dealt with by ineffective self regulatory codes imposed by the direct marketing industry or ISPs. Both European governments and the EU must actively seek American support and co-operation, in this area as in the field of data protection, if what is effectively an American vice is not to be exported without impediment to the rest of the world (101). However the recent protracted and halting status of negotiations between the EU and the US on trans-border data flows and "safe harbour" provisions does not inspire great sanguinity that this approach will bear fruit in a hurry (102). In the end it may be that as with other vices currently afflicting the Internet such as child pornography, the way forward for the EU nations is some kind of concerted Action Plan by virtue of which hard cash is put on the table, not only to improve technical fixes, but also to provide public education as to what opt-out (and one hopes, in future, opt-in) schemes are available to empower consumers to avoid unsolicited commercial communications of all kinds, and to support ISPs, such as America Online in the States, who are prepared to go to court to protect their client base and reputation from the tinge of spam. This has merely been a progress report on the long road to stamping out spam.

Footnotes

1. Senior Lecturer, The School of Law, Edinburgh University. E-mail: L.Edwards@ed.ac.uk. My grateful thanks to John Dallman, who provided useful information in relation to technical fixes for spam, and also to Mark Lemley and Geraint Howells for their helpful comments and advice.
2. The name "spam" is, as a matter of Internet urban myth, supposed to derive from a well known Monty Python TV comedy sketch involving the chanting of"spam, spam, spam" over and over again.
3. An interesting non legal account of the genesis of spam can be found in "Make.Money.Fast" in W.Grossman Net.Wars (NYUP, 1997).
4. This is the informal title of a US Bill introduced into the House of Representatives by Congressman Miller on 10 June 1999.
5. Tentative but growing legal interest in the UK can be seen taking visible shape in the form of a number of short articles and industry reports, nearly all of which seem to be entitled "A Spammer in the Works"; cf. Onwusah (1998) 148 NLJ 1718; Drew (1998) 9 Computers and Law 13; Mackay, 4 May 1999, Scotsman Interactive section; Novell report commissioned from Benchmark Solutions on impact of spam on UK industry, reported in Scotsman, 29 April 1998. This author has resisted the temptation to continue in this grand tradition. An industry based pressure group, associated with the US body CAUCE, the Coalition against Unsolicited Commercial Email, has recently been formed in Europe to resist spam : The European Coalition Against Unsolicited Commercial Email, web site at http://www.euro.cauce.org/en/index.html. The UK pages are to be found at http://www.euro.cauce.org/en/countries/c_uk.html. CAUCE's web site can be found at http://www.cause.org. Another useful US anti-spam site is Junkbusters at http://www.junkbusters.com .
6. See further below, ppxx.
7. Dallman and Dowling note "The British Government is shortly due for a nasty shock due to their policy of connecting all schools to the Internet. Imagine the reaction when the tabloid press discovers that schoolchildren are being sent advertisements for pornography via the email accounts that the government has provided." Towards Useable Email, p 2 at http://www.davros.org/legal/dmaspam.html.

8. See Byrne "Squeezing Spam Off the Net : Federal Regulation of Unsolicited Commercial Email" (1998) 2 W,Va. JL and Tech 4.
9. Although this is a less serious issue in the USA where local calls are free, and, increasingly, is also diminishing in significance in the UK as freeserves and flat rate schemes such as that provided by NTL have become available.
10. See especially the EC Electronic Commerce Directive, Arts 6 and 7, originally proposed on 18 November 1998, available at http://www.ispo.cec.be/Ecommerce/legal.htm#legal (COM(1998) 586 final), and the commentary thereto. Final Act reached 8 June 2000.At the time of writing the final version of this Directive is not available on the Web; the version used is as of 8 May 2000 OJEC Volume 43 2000/C128/02
11. See further Akdeniz, pXX; Hogg, p xxx.
12. Dickie has described this as a "market" rather than a "welfarist" focus in regard to regulation of the Internet: see Internet and Electronic Commerce Law in the European Union (1999, Hart Publishing), p 101.
13. The Report to the Federal Trade Commission of the Ad Hoc Working Group on Unsolicited Commercial Email (http://www.cdt.org/spam) estimated that around a half of unsolicited commercial email messages contained fraudulent or deceptive content, and of the other half, much contained inaccurate email header information ie, misleading subject lines or sender.
14. Report commissioned from Benchmark Solutions by Novell on impact of spam on UK industry, reported in Scotsman, 29 April 1998
15. Compare the international furor caused, when Microsoft were forced by hackers to shut down the free web based email system Hotmail for a few hours as a result of its compromise by hackers. See http://news2.thls.bbc.co.uk/hi/english/sci/tech/newsid%5F434000/434120.stm.
16. AOL v Prime Data Systems Inc ED Va No 97-1652-A, 12/10/98.
17. Compuserve Inc v Cyber Promotions Inc No C2-96-1070 (SD Ohio 24/10/96).
18. Most email programs have a simple command which allows a "reply-to" address to be set which has no relation to the actual address of sender. Ironically, such tactics are sometimes used by spam-avoiders to avoid giving a true reply address out to the world which spammers can then harvest.
19. In a brief survey of contracts of six leading ISPs in the UK market, four (Demon, Virgin, Freeserve and Sharkhunt) imposed anti-spam clauses in their subscriber contracts. Interestingly, the ISP Association, a UK industry body, has adopted a voluntary Code of Practice as of 25 January 1999 which requires ISP members to follow best industry practice in using anti spamming software so that customers can elect to minimise the amount of spam they receive, but does not require an anti-spam termination clause (para 7.1.6).
20. See Murray, pXX . In a recent Canadian case, 127623 Ontario Inc v Nexx Online Inc, Court File No C20546/99, (Ontario Superior Court of Justice, June 14 1999), an ISP had no explicit anti-spam clause in the hosting agreement, but did have a clause requiring compliance with "generally accepted netiquette". The court held this entitled the ISP to terminate the agreement when it discovered its client was an active spammer.
21. Although as seen above there is a reasonable body of knowledge about how costs of spam can be pre-estimated. See further Stair Memorial Encyclopaedia, Vol 15, pp 510ff, and Dunlop Pneumatic Tyre Co v New Garage & Motor Co [1915] AC 79.
22. See r 2(1) and 3(1) of the Regulations. Under UCTA77, however, terms in a standard form contract are subject to review by the court if they allow one party to offer a performance substantially different from that which the other party reasonably expected under the contract, even if the contract is made business to business (1977 Act,17(1)(b)).
23. See further "Virgin Sues Spam Man", BBC News, at http://news2.thls.bbc.co.uk/hi/english/sci/tech/newsid%5F323000/323817.stm.
24. See E-Commerce Law and Policy, June 1999, Vol 1, issue 5.
25. Although he subsequently set up three more accounts with Virgin under false names.
26. A notable recent success story using this approach is Earthlink Networks v Cyber Promotions, No BC 167502 (Cal.Super. Ct.LA County, March 30 1998) where the ISP achieved a $2m settlement against the spammer. See also AOL Inc v IMS 1998 US Dist LEXIS 17437 (ED Va. October 29 1998) .
27. Supra n 16.
28. See Winfield and Jolowicz on Tort (Sweet & Maxwell,1998,15th edn) pp583-588.
29. Supra n 22.
30. See Thomson Delictual Liability (1994, Butterworths) p 21 citing Leitch v Leydon 1931 SC (HL) 1; Walker on Delict, Vol II (W.Green&Co, 1966) pp 938ff.
31. See further Thomson, supra n 28, pp 1 and 22ff on the use of culpa to cover intentional and unintentional wrongs. However it is clear that historically Scots law used culpa only for negligent acts and dolus for intentional wrongs cf A. T. Glegg, A Practical Treatise on the Law of Reparation (1st edn, 1892) 8, 12, 34-5.
32. See Torquay Hotel v Cousins [1969] 2 Ch 106.
33. See Lonhro plc v Fayed [1990] QB 490 and Thomson,supra n 28, pp 38-39; Stair Memorial

Encyclopaedia, Vol 15,pp 380ff; Winfield and Jolowicz, supra n 27, Chapter 18.
34. See further Waelde, pxx.
35. Supra n 16. See also Hotmail Corp v Van$ Money Pie Inc 47 USPQ 2d 1020 (ND Cal 1998) (also at (1998) 3 BNA ECLR 586); AOL v IMS 1998 US Dist Lexis 17437 (ED Va. October 29, 1998).
36. Yahoo!, commenting on their successful suit for trademark infringement against spammers in Yahoo! Inc v World Wide Network Marketing ND Calif No C-99-20234 (14 April 1999),reported at (1999) 4 BNA ECLR 384.
37. See further Law Commission Report No 186 Computer Misuse Cm 819.
38. See Scotsman, Interactive section, ?? 1998.
39. v[1998] Masons CLR, Rep 141.
40. See further s 3(1)(b) and (3) of CMA, and below. The intent need not be directed at any particular computer or any particular program or at securing any particular modification.
41. Although they can contain programs eg attached exe files.
42. The Concise Oxford Dictionary, 7th edn, defines data as the plural of datum, and that, inter alia, as "facts or information, especially as basis for inference; quantities or characters operated on by computers etc and stored or transmitted on punched cards, etc."
43. There is also an interesting reductio ad absurdam result to this argument in that entirely legitimate Internet users who are not subscribed to an ISP but send email to users who are clients of that ISP are as likely as spammers to be guilty of an "unauthorised modification" - hence sending email would in principle be potentially criminal under s 3!
44. To secure a s 3 conviction, the spammer must also know their modification was unauthorised - s 3 ((2) and (4).
45. See the Thefts Act 1968 and Smith and Hogan on Criminal Law (Butterworths, 8th edn, 1996).
46. In Art 8.
47. Virginia State Board of Pharmacy v Virginia Citizen's Consumer Council Inc 425 US 748.
48. 95/46/EC, OJ 1995 L281/31.
49. See further, Charlesworth, pxx.
50. A useful concise analysis of how the 1998 Act relates to the Internet can be found in Millard "Data Protection and the Internet" (1999) 9 Computers & Law 29.
51. 1998 Act, s 4(4).
52. Ibid, s 17(1).
53. Ibid, s 13.
54. Ibid, s 21. I
55. Ibid, s 1(1)).
56. Laws of the Internet (Butterworths, 1997), p 253.
57. Although this might not always hold true : if eg the spammer was seeking to send spam concerning pornography only to males between 18 and 50. The economics of spamming however - ie its cheapness, however many are spammed - tend to make selection amongst those targetted for particular groups unlikely.
58. 1998 Act, Sched 2, para 6(1).
59. Carey Blackstone's Guide to the Data Protection Act 1998 (Blackstones, 1998).
60. "Direct marketing" is defined for these purposes as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals" (s 11(3) and so includes spam as well as traditional junk mail.
61. 1998 Act, s 5(1).
62. Although to some extent these extra-EU enforcement problems are being addressed, if slowly, in relation to trans-border data flows to the USA (see Charlesworth, pXX).
63. 1998 Act, s 40.
64. Directive 97/7/EC, OJ No L 144/19.
65. However as of June 26 2000 no regulations had yet been implemented by SI in the UK. See the progress report at http://www.dti.gov.uk/CACP/ca/dsdbulletin.htm .
66. Art 10(1).
67. See Art 2 and Annex 1, which specifically refers to "electronic mail".
68. See the November 1999 DTI consultative document Distance Selling Directive - Implementation in the UK and attached draft regulations at http://www.dti.gov.uk/cacp/ca/distance/dist.htm .
69. Ibid. .
70. However the draft EC Directive on Distance Marketing of Financial Services (COM (1998) 468) will fill this gap.
71. SI 1998 No 3170.
72. 97/66/EC. The Regulations came into force on 1 May 1999.
73. See Telecoms Data Protection Directive Implementation In the UK - Draft Regulations, para 2.3 at http://www.dti.gov/CII/tdpd/condoc2.ytm.
74. See Building Confidence in Electronic Commerce, 5 March 1999, para s 28-31, at http://www.dti.gov.uk/CII/elec/elec/elec_com.html.
75. See Art 12(1). It is noteworthy that even in the US, the home of free speech, automated calling machines are banned (although enforcement of this is patchy) and this ban has been upheld as

constitutional (see Moser v Fderal Communications Commission 46 F.3d 970 (9th Cir. 1995).

76. The November 1999 consultation on implementation of the Distance Selling Directive (supra) does seem to move closer towards a view that spam should be classed as more invasive and annoying than ordinary hard copy unsolicited communications, and therefore more appropriately controlled by an opt-in regime.
77. This point is made by Clive Feather of Demon Internet in his response to the DTI consultation document, supra, no 61. See http://www.davros.org/legal/ecommsub.html.
78. Supra, n 10. At the time of writing the final version of this Directive is not available on the Web; the version used is as of 8 May 2000 OJEC Volume 43 2000/C128/02.
79. The Draft Directive suggests that such information might satisfactorily be provided by a hyper link in the case of a web page making a commercial communication; such a link could also be placed in an email.
80. Supra, n 61.
81. See http://www.dti.gov.uk/CII/elec/conrep.htm at para 24.
82. Ibid, in "Notes on responses to specific questions".
83. The Committee on Culture, Youth, Education and the Media also recommended an amendment to the Directive which would have required prior consent from consumers to unsolicited commercial communications; however this was not adopted.
84. See Edwards, pxx; Akdeniz, pxx.
85. Supra, n 14.
86. Some European states, notably Germany and Austria, have however passed legislation which explicitly makes it illegal to send unsolicited email.
87. A full list of US state legislation in this area can be found at http://www.jmls.edu/cyber/statutes/email/state.html.
88. House Bill 2752, subsequently amended by HB 1037.
89. The Washington State anti-spam law was however declared invalid on March 10 2000 as violating the interstate commerce clause of the US Constitution by being "unduely restrictive and burdensome", the claim upheld being that the law restricted legitimate business more than it aided consumers. An appeal is in progress.
90. However this statute was also ruled unconstitutional on 19 June 2000 by a San Francisco state court (Ferguson v Friendfinder.)
91. See further Byrne, supra n 8, and Goldstone "A Funny Thing Happened on the Way To The Cyber Forum: Public v Private in Cyberspace Speech" (1998) 69 U of Colorado Law Rev 1. It has been held that it is not an unconstitutional infringement of the right of free speech for an ISP to take steps to filter out or prevent spam arriving in mailboxes: this is because an ISP is a private actor, not an organ of the state, See Cyber Promotions Inc v AOL CA No 96-2486, November 4 1996.
92. Arts 28 and 49 of the EC Treaty.
93. See ns 89 and 90 above.
94. See Dallman and Dowling, supra n 7.
95. Run by the Mail Abuse Protection System (MAPS). See further http://maps.vix.com.
96. Both Harvard University and Virgin Net have at one time been listed on the Real Time Black Hole List.
97. For example, Pegasus Mail, a mail program used extensively in universities, affixes information to the header of any email mesage sent to more than 50 recipients, indicating if it is "moderate", "bulk" or "mass" distribution. Systems administrators on receiving networks can then use their filtering tools to reject any message sent to more than a certain number of recipients.
98. Unfortunately the commonest email server software, Microsoft Exchange, is currently not configurable to reject falsified addresses.
99. For the ISP Association's approach, see supra n 21.
100. See http://www.ja.net/documents/use.html.
101. It is worth noting however that a determined victim of spamming can take the fight to the US courts. The UK Internet company Bibiliotech sued spammer Sam Khuri in the US and in March 2000 were awarded undisclosed damages plus a ruling that Khuri would have to pay $1000 dollars to any future person spammed. This is the first case involving a European company brought against a spammer in the US courts.
102. See further Charlesworth, Chap X.